CLAIMS

We claim:

1. A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network, said packet filter not responding to said external network upon receiving requests from said external network to access said internal network; and,

a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network.

2. The stealth firewall of claim 1, wherein said requests from said external network comprise transport control protocol (TCP) SYN messages.

3. The stealth firewall of claim 2, wherein each state in said state machine corresponds to data in a specified field of said TCP SYN messages.

4. The stealth firewall of claim 3, wherein said specified field comprises a destination port field.

5. The stealth firewall of claim 1, wherein said code is a rolling code which can vary according to time.

6. The stealth firewall of claim 2, wherein said packet filter can permit access to a specific port in said internal network based upon a destination port specified in a TCP SYN message received after transitioning to said access state in said state machine.

7. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access

parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

8. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

9. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.

10. A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network, said packet filter ignoring requests from said external network to access said internal network;

fixed storage in which at least one authentication password can be stored;

a hash processor configured to apply a hashing algorithm to said stored at least one authentication password; and,

a comparator configured to compare a hashed password and timestamp received from said first network interface, with a hashed result produced by said hash processor for a stored password associated with a user at said first network interface, said comparator causing said packet filter to permit access to said internal network where said hashed password and timestamp matches said hashed result.

11. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

12. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

13. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.